Cyber Security Status

Presentation to RHIC/AGS UEC Meeting

Thomas J. Schlagel
Information Technology Division
January 23, 2004

DOE Audit History

- DOE Office of Oversight and Performance Assurance (OA) Cyber Security Inspection, 3/2000
  - 6 Findings; **Unsatisfactory** Rating
- DOE Chicago Operations Office (CH) Cyber Security Review, 4/2001
  - 12 Recommendations; No change to **Unsatisfactory** rating.
- DOE CH Safeguards and Security Inspection, 12/2001
  - Closure of one finding from March 2000 OA and six recommendations from 6 April 2001 CH; No change to **Unsatisfactory** rating.
- DOE CH Letter Dated October 21st, 2002
  - Closure of remaining 5 findings from March 2000 OA inspection
- Cyber Security Peer Review, 11/2002
  - Six findings, seven recommendations
- Five recommendations from 4/2001 CH Review closed
  - One remaining open recommendation - implementation of DOE N205.2, “Foreign National Access to DOE Cyber Systems”
- DOE Chicago Operations, 11/2003
  - Three new findings; Upgraded to **Marginal** Rating!
- ➢ Next Review – DOE OA Cyber Security Inspection
  - Originally scheduled for March 2004; Rescheduled for November 2004 – waiting for confirmation

Need to respond to findings from Chicago Ops inspection and prepare for OA Inspection this November.

DOE Findings/Recommendations

Findings/Recommendations	Issues
1. Poor Network Mgt. Practices • Very Weak Perimeter (no firewall) • No Knowledge of Connections	• Active unused jacks that are unmonitored • Lack of Configuration Management (no controls; need more understanding of computer hardware & software on the network. • Lack of guidance regarding security of computer systems (properly configured and contain the most recent patches)
2. Inconsistent Cyber Security Banner	• Users may not be informed that their actions are subject to monitoring
3. No Roles, Responsibilities, Authorities, & Accountabilities	
4. No Risk Assessment Process	•For systems and enclaves not controlled by ITD •(OA & CH)
5. No Effective Procedures	
6. No Self-Assessment Process	
7. Implement Password Procedure	
8. Address Perimeter Vulnerabilities	

DOE Findings/Recommendations (cont.)

9. Develop Secure Configurations	
10. Implement CSIRT Procedure (Establish Authority)	
11. Document External Connections	
12. Evaluate Effectiveness of Internal Network Zones	
13. Define Line Management Responsibilities	
14. Set Up Security Logging and Monitoring	
15. Track Foreign Visits and Assignments	Access control - remote & direct users

Findings from DOE Chicago Operations Office Safeguards and Security Inspection of BNL, September 22-26, 2003

1. *BNL has not consistently reported Cyber Security Incidents to DOE line management in accordance with established procedures and the approved CSPP.*

2. *BNL has not completely implemented DOE N205.2 "Foreign National Access to DOE Cyber Systems". An approval process based on risk assessment has been applied to critical systems and some other laboratory cyber systems, but there are not specific approvals for access to the majority of site systems.*

3. *BNL has not consistently protected cyber assets in accordance with risk analyses*
   - *Open Wireless Access Points (WAPs)*
   - *Windows system with a file share open to the Internet*
   - *Cyber Security Incident involving a computer system inappropriately placed on a subnet open to the Internet*

Configuration Management Audit Findings

- Issues of concern on 30% of 190 systems identified by *external* scans
  - Lack of latest security updates on 21 of 89 web servers
  - Lack of appropriate warning banner on 21 of 39 FTP servers.
- Issues of concern on scans of *internal* network – poor configuration management
  - Systems with large number of unnecessary services, including clear text services
  - Numerous software vulnerabilities
- WAP survey
  - 67 wireless access points detected
  - 28 employed encryption
  - Connectivity was achieved with 9 WAP's, with 3 providing access to the campus network

Poor Configuration Management remains the most serious deficiency of the BNL Cyber Security Program

Cyber Security Working Groups

- Cyber Security Advisory Committee met December 10 to discuss audit findings and corrective action plans. Meeting again on February 4.
- Formed three working groups composed of ITD, CSAC and system administrators. Recommendations due back in mid-January, presented to CSAC on February 4
  - Foreign National Access to cyber systems
  - Wireless networking
  - Configuration management
- Revised Corrective Action Plan due to Chicago Ops on February 10th

Recommended Actions (presented to CSAC)

Finding 1 – Action:

- Establish protocol for Federal line management reporting with BAO

Finding 2 – Action:

- Develop straw man Configuration Management Guide
  - Devices connecting to the network
    - critical servers, financial systems, Exchange
  - System deployment - standard security checklists
    - Windows, Unix, MAC
  - Auditing (scanning and reporting)
  - Consequences for non-conformance of Configuration Management Policy
    - e.g, ES&H Violations
- Volunteers for Working Group to develop configuration management guide

Recommended Actions (cont)

Finding 2 – Action (continued.)

- Wireless Policy Review
  - Visitor Network vs. Campus Network or both?
    - Some add on security component – Authentication?
  - APs request through CSMIS or Registration Network DB before deployment
  - APs should be Enterprise class network equipment to enable network mgmt and upgrades
    - Advantages:
      - Contact the Help Desk
      - Wireless trouble calls
      - System support services, e.g., installing WLAN cards, laptop problems
      - Wireless support pages (www.bnl.gov/itd)
  - Study to determine exact risks and details of risk mitigation
  - Volunteers for working group to develop policy and procedures

Recommended Actions (cont)

Finding 3 – Action:

- Need to improve BNL's list of sensitive computer systems to include all computers used in unclassified but sensitive programs (e.g., Cradas).
- On-site access
  - Foreign nationals complete I-473 form before arrival at BNL
  - Designated official to approve access to computer systems
    - Blanket approval to open systems (email, desktop, servers, ...)
    - Specific approval to sensitive systems if required. This will be an extension of existing procedures for access to sensitive information.
  - Access will be granted for a period not to exceed duration of foreign national's appointment.
- **Remote-only access**
  - **Need to develop an on-line application form for remote users**
  - **Approval process as for on-site access**
  - ***What about Grid users?***
- Establish automated procedure to monitor who has accounts on computers
  - Accounts already monitored on most critical and sensitive systems
  - Expand to newly identified critical and sensitive systems and to major servers
- **Form working group to develop policies and procedures**

Recommended Actions (cont)

- We need a thorough review of all cyber security policies and responses to previous findings to make sure that we are still in full compliance.
  - *We must do what we* ***say*** *we are doing.*
- Need to establish clear metrics so that we can clearly judge the success of our cyber security program – one component of a successful management system

DOE OA Inspection of PNNL - Summary

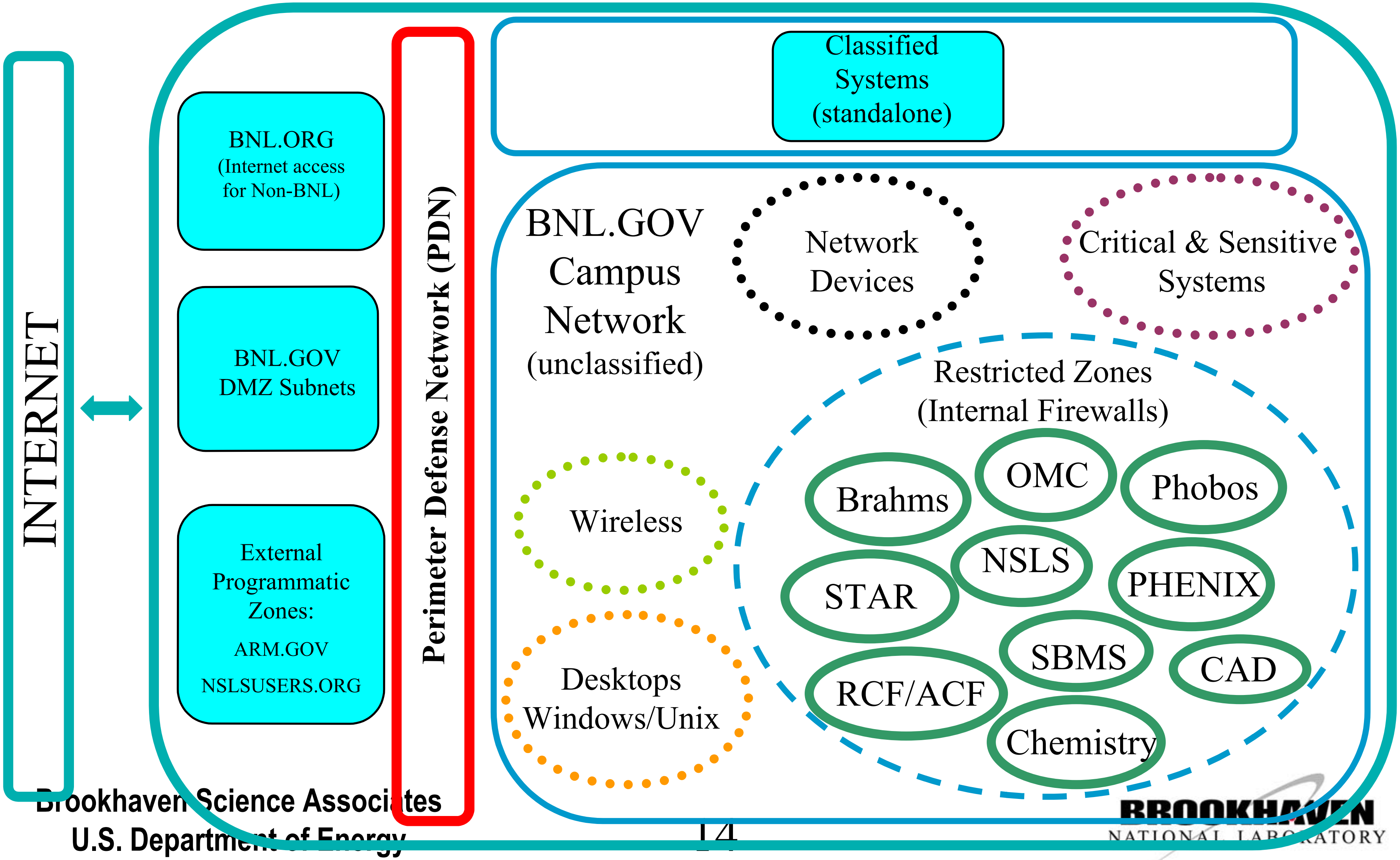
Concerns: (OA Findings against PNNL – received Unsatisfactory in audit last year)

- ➢ Lack of documentation describing specific threat - If it isn't written it doesn't exist
- ➢ Monitoring foreign national access
  - Eliminate any root level or admin access for foreign nationals
  - Lack of Tracking of foreign national use
  - Foreign national access to sensitive data – any kind (written up)
- ➢ Scanning for vulnerabilities, patching, rescanning to assure patching on each specific system was performed
- ➢ Open high ports are a problem (?)
- ➢ Lack of IDS coverage inside for protection against the insider is an issue
  - Installing Snort IDS sensors to alert on suspicious campus traffic on selected subnets with ability to change the subnets selected
  - Centralizing reporting of host logs allowing a unified view of activity regardless of source
  - Both projects are ongoing with data being collected
- Data could be stolen while it is in memory (?)
- No credit for planned work even if the implementation was in process

Risk Assessments

- Formalize risk assessments for cyber enclaves:
  - *"A cyber enclave is an interconnected information resource with a common level of functionality under a defined management structure. The cyber enclave normally incorporates hardware, software, information, data, applications, communications, facilities, staff and provides capability and functionality for a prescribed set applications and users."*
- Risk process includes identification and assessment of:
  - Threats
  - Vulnerabilities
  - Costs to mitigate vulnerabilities
- Document and accept residual risks
- Risk assessments signed off by Laboratory director

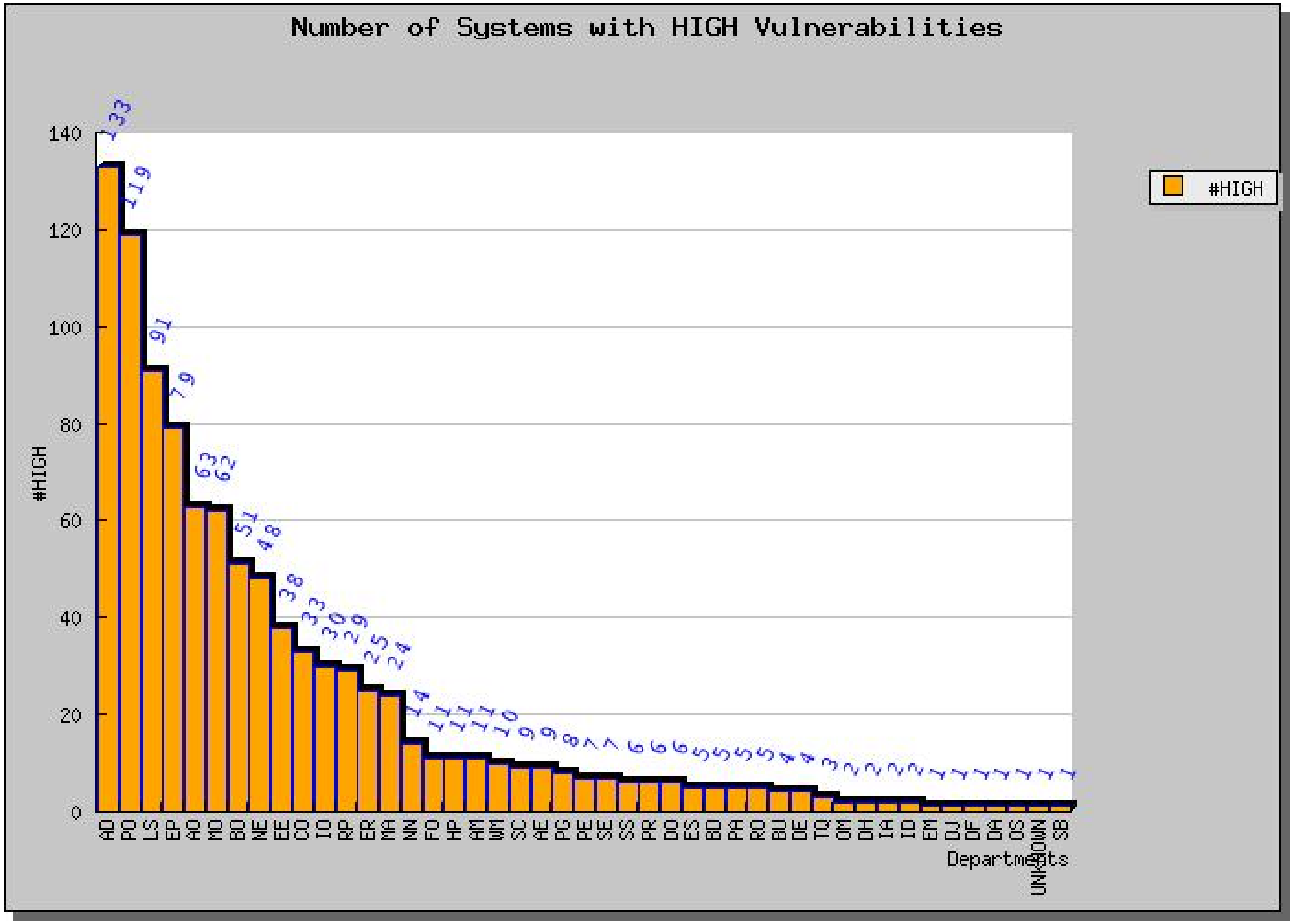
BNL Cyber Enclave Topology



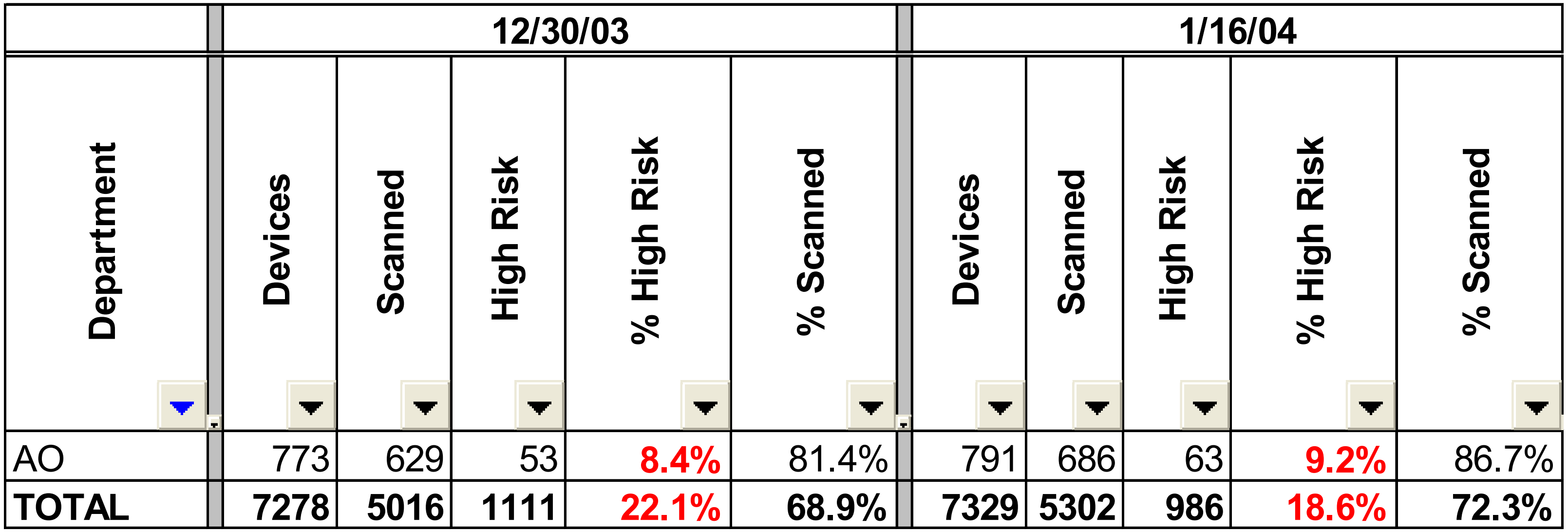
Vulnerability Scanning

- BNL uses *nessus* security scanner (www.nessus.org)
  - Scanner tries to connect to devices in BNL IP address range
    - Internal scans – BNL.GOV campus network + internal firewalls
    - External scans – Anything in the BNL.GOV visible from the Internet
  - Connect to ports and attempt to identify services
  - *nessus* maintains a database of signatures for services with security vulnerabilities, and categorizes them as low, medium and high.
- Database maintains list of "false positive" – vulnerabilities that have been corrected, but that nessus still flags (due to the fact that signature is the same)
- ➢ Need to add flag to categorize vulnerability as "uncorrectable" – software cannot be upgraded, or service is needed and vulnerability is acceptable risk, but not a false positive.
- ITD scans systems quarterly – last scan completed January 15th with exception of one department and behind some firewalls.
- Asking system administrators to address high security vulnerabilities – will rescan after 2 weeks to measure progress.
- Systems scanned after initial registration – not currently being done
- Need automated scanning behind firewalled enclaves; enclave schedules and runs
- Just began cross-referencing vulnerability scan results with Network Registration database to get useful summaries: By Department, By Operating Systems, By Service, By Vulnerability

Systems with high security vulnerabilities



Vulnerability Scanning Metrics



Department	12/30/03					1/16/04				
	Devices	Scanned	High Risk	% High Risk	% Scanned	Devices	Scanned	High Risk	% High Risk	% Scanned
AO	773	629	53	8.4%	81.4%	791	686	63	9.2%	86.7%
TOTAL	**7278**	**5016**	**1111**	**22.1%**	**68.9%**	**7329**	**5302**	**986**	**18.6%**	**72.3%**

Devices - # devices in Network Registration database (IP)

Scanned - # devices seen in last scan

High Risk - # devices with high risk vulnerabilities as determined by nessus

% High Risk - % of devices with high risk vulnerabilities to total number of scanned devices

% Scanned - % scanned devices to total number of registered devices

IDS and WAPs

IDS and Log Analysis

- Analysis of firewall and system logs to look for signs of probing, denial of service or break in.
- Goal is to have all systems with conduits in the PDN firewall, and critical/sensitive systems logging to the central log server.

Wireless Access Point (WAP) Detection

- Air Defense pilot rollout to determine effectiveness at detecting wireless access points. Full deployment on successful pilot. Product also being piloted at PNNL.
- "War Driving" – manual detection of WAP's with antenna will commence on a regular basis to detect access points. When Air Defense is successfully deployed across the campus, war driving can cease.

Configuration Management Tools

Windows

- Microsoft Software Update Services (SUS) installed on all Windows XP and 2000 systems
- SMS pilot for Windows administration on 100 systems. Budgeting for EU license to run on most Windows systems at the lab. This could eventually replace SUS on most Windows systems.

Redhat Linux

- Deployed RHEN Satellite Server last week, purchased 350 copies of RHEL 3.0. Satellite Server allows easy patching of RH systems; ability to deliver custom configurations; central database with system information including list of installed patches

Virus Protection

- BNL uses products from **Trend Micro** for desktop, server, and e-mail protection; **f-prot** on Internet e-mail gateways – also flags SPAM.
- Over 95% of Windows systems on the network are running Trend Micro antivirus software. Cyber Security group continually watches for machines that pop up without AV protection, contacts users with infected machines.
- eShield product installed in December. Used to block viruses from computers connecting via dial up (IDAS).

Miscellaneous

- Password cracking notification process
  - Cross reference BNL NT Domain account information with LDAP to get contact info for users.
- Registration database cleanup
  - Contains contact, location and department info for all registered systems on site – but data has not been maintained – needs to be scrubbed.
- Web documentation cleanup
  - Difficult to find relevant information. Being done as part of the CM process.

How Can You Help?

- All computer systems must have DOE Security Banner installed.
- All PC’s run Trend Micro AntiVirus software.
- All Windows 2000 and XP systems running Microsoft SUS to get critical and security updates
- All users update network registration database when there are changes to
  - operating system; contact and administrator information; location
- All system administrators
  - Review system configurations to make sure that they meet security checklists – no unnecessary services, turn off clear text services whenever possible
  - Patch systems (especially UNIX/LINUX) regularly
  - Respond to vulnerability scan reports, address vulnerabilities rated “high”
  - Register and ensure proper access control on WAP’s.